数据伞内网信息保护软件 V5.0
使用手册

青岛城市规划咨询公司

服务电话：0532-83863512

目录

一 前言

欢迎您使用数据伞内网信息保护软件，请您仔细阅读以下信息：

产品信息

完整的数据伞内网信息保护软件包装盒应包括以下物品：

1. 数据伞内网信息保护软件安装光盘；
2. 用户手册一本；
3. 加密狗一个；

如果您购买的数据伞内网信息保护软件缺少上述任一物品，请及时与供货商联系。

信誉保证

如果您在使用过程发现了什么问题，请及时拨打供货商电话联系，或者参考说明书相关章节寻找解决办法。

如果您对我们的产品有什么意见或者建议，也请不吝指教，以便我们不断改进。

版权声明

授权说明

在安装本软件产品之前，请仔细阅读下列内容，如果开始安装，则表示同意以下全部条款，本许可协议即开始生效。

1. 本软件版权为**青岛市城市规划设计研究院**和**北京世优时代科技有限公司**共同所有，任何人无权对本软件的任何部分进行修改、分解、反汇编和反编译。
2. 本软件是已经注册登记并受法律保护的商业软件，它的适用法律包括《中华人民共和国计算机软件保护法》《中华人民共和国著作权法》等。
3. 您将本软件转让他方使用时，请务必将本许可协议一并转让，并销毁在计算机上和各种介质上的相关备份，您的许可权即终止。

二 运行环境要求

2．1 软件要求

操作系统要求 Win2000/WinXP/Win2003。（其中，推荐将服务器程序安装于 Win2003 或 Win2000 Server 上）

2．2．硬件要求

服务器端：CPU 2G 以上，内存 512M 以上，硬盘空间 500M 以上。

客户端及领导控制台：能正常安装和使用 Win2000/WinXP/Win2003 的计算机即可。

三、软件安装

3.1、服务器端安装

3.1.1：得到“数据伞内网信息保护软件”的安装程序

完整的安装程序包括两个可执行程序（3.1-Winpcap．exe 和 SFG．exe）；

3.1.2：安装网络支持包“3.1-Winpcap．exe”

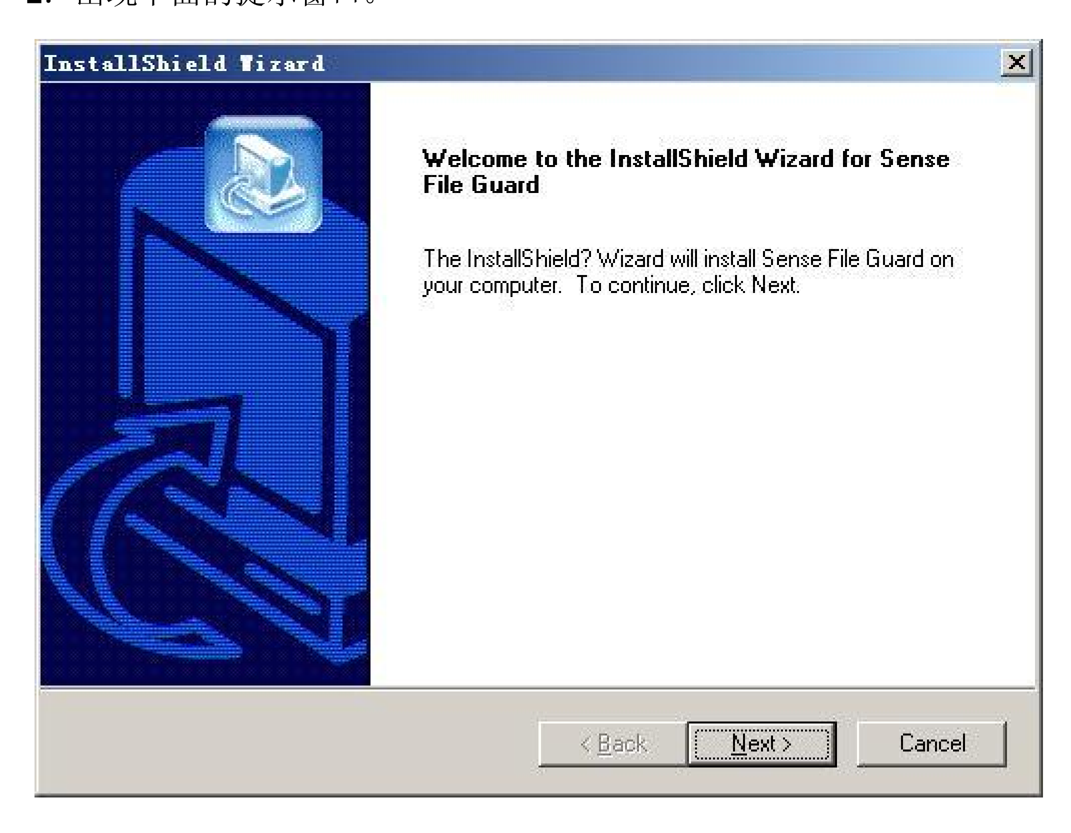
在安装服务器程序的计算机上安装网络支持包“3.1-Winpcap．exe”(根据安装向导一直按默认提示安装即可)；

3.1.3：安装服务器程序

1．在安装服务器程序的计算机上找到服务器端安装程序文件“SFG.．exe”并双击，开始进行安装。



2．出现下面的提示窗口。



3．单击【下一步】，出现使用协议界面。



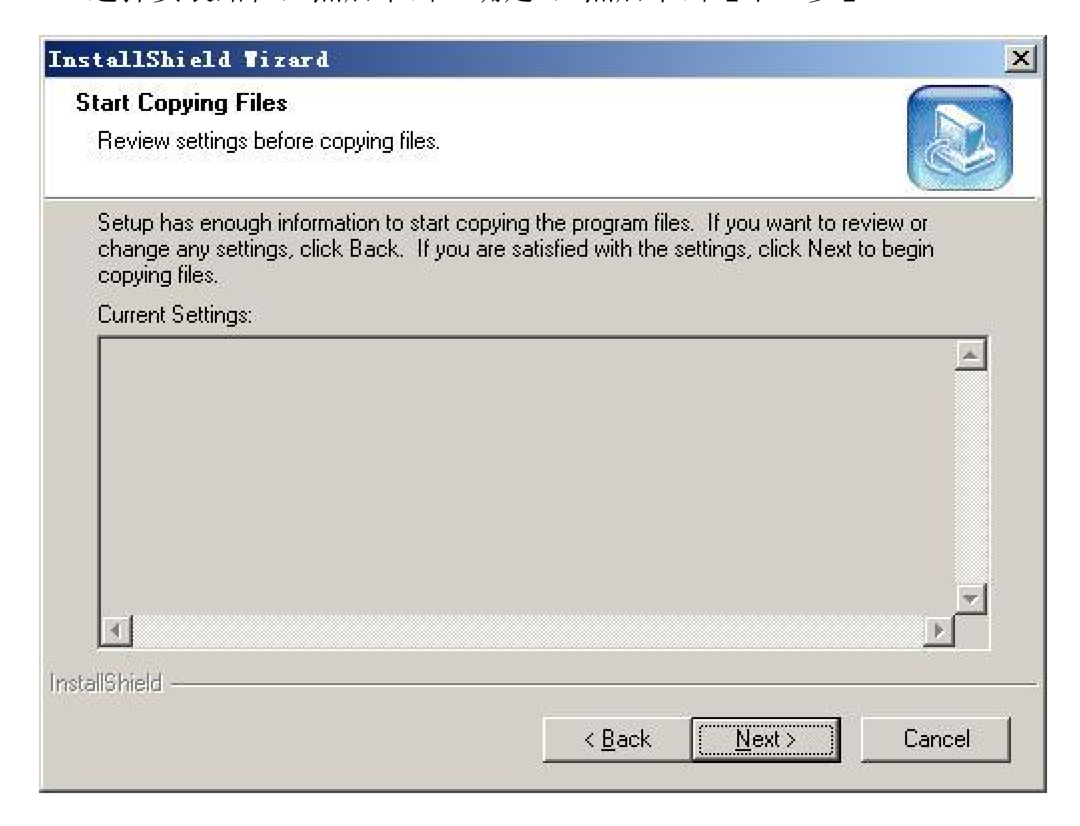
4．单击【同意】，出现选择安装路径界面。



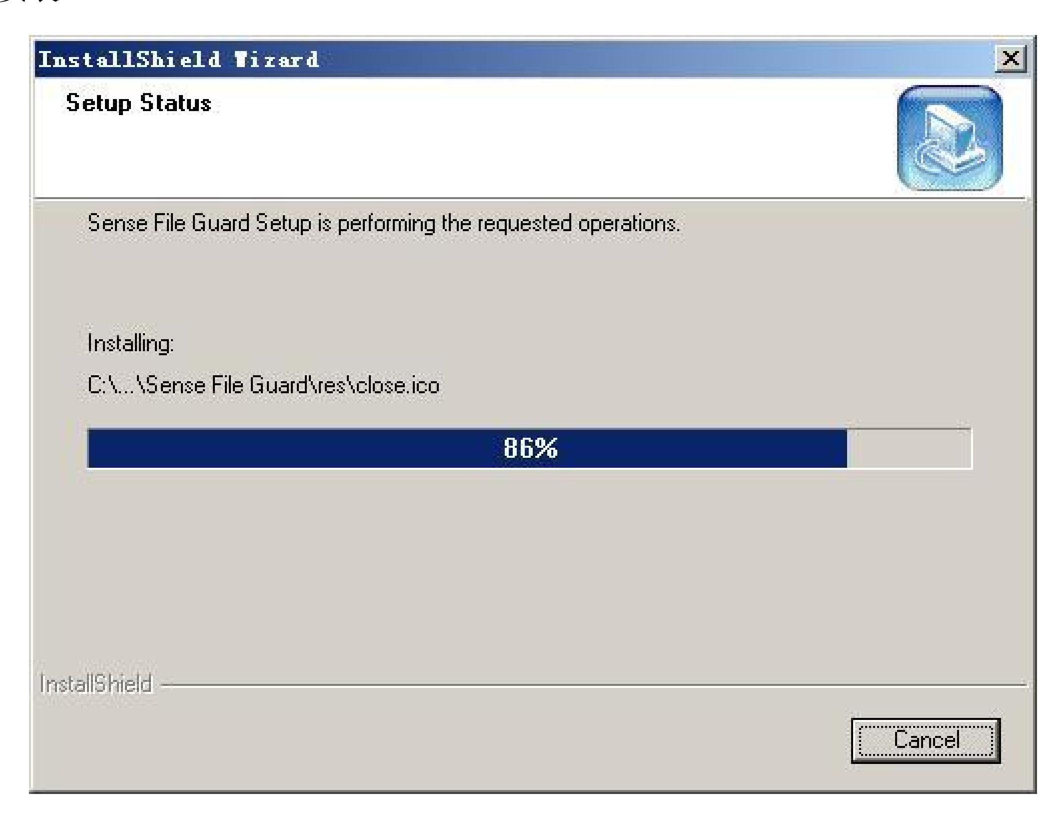
5. 单击【浏览】，弹出目录选择窗口如下。



6. 选择安装路径，然后单击“确定”，然后单击【下一步】。



7. 单击【下一步】，安装程序开始进行安装，安装向导将自动完成服务器端的安装。



8. 安装程序开始进行安装，安装向导将自动完成服务器端的安装。



3.2、客户端及管理工具安装

3.2.1、生成客户端及管理工具安装程序。

运行服务器程序（服务器程序安装成功后会在桌面开始菜单中创建快捷方式），通过服务器程序的主界面上方的“生成客户端”按钮即可生成客户端安装程序 V1.000.exe、领导控制台程序（领导控制台.exe）、管理员工具（管理员工具.exe）。

客户端及管理工具程序说明：

1）客户端安装程序 V1.000.exe，用于安装至各需要受监控的主机上(注：安装服务器的主机最好不要安装客户端程序，这样会影响服务器的性能)；

2）领导控制台.exe：给领导专门使用的控制台程序，领导通过此程序即可实时监控所有的被监控主机；

3）管理员工具.exe：给系统管理员专用的工具（请不要随意放置），其功能包括，如：停止客户端运行，卸载客户端，，启用安全模式，禁用安全模式等。

3.2.2、安装客户端程序

1、点击户端安装程序 V1.000.exe，出现以下界面：



2. 点击“注入”按钮即可成功自动成功安装客户端。

注：客户端安装完成后，在以后每次开机时会自动在后台运行，且在进程管理工具中不可见，要卸载/停止或其它的维护需要通过系统管理员工具才行。

3.2.3、安装领导控制台

领导控制台无需安装，直接复制并放到领导计算机的桌面上，使用时直接运行这个程序即可。

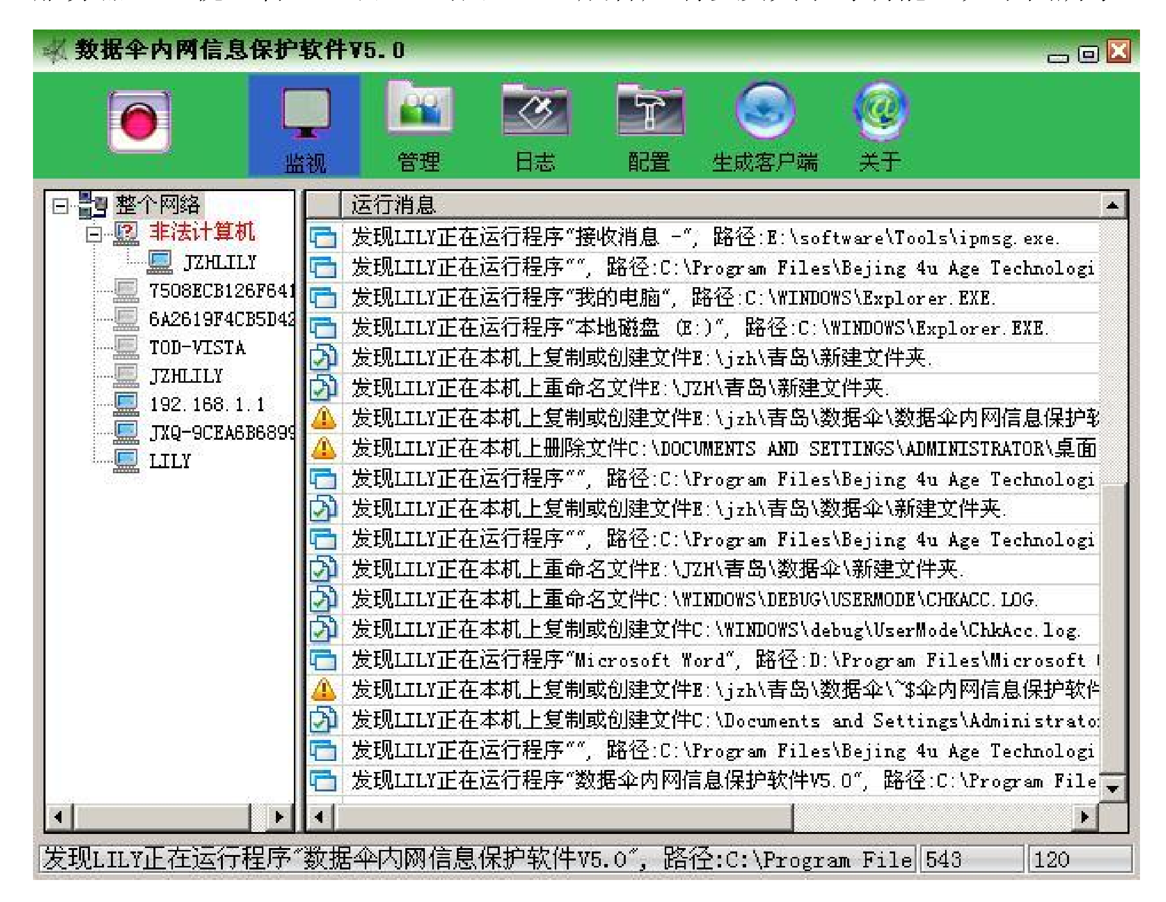
3.2.4、安装管理员工具

管理员工具无需安装，并且此工具不能外泄，为管理员专用。

四、功能菜单

4. 1、服务器端程序主界面

服务器端可以监控在整个局域网中所有计算机文件操作情况，主要包括启动服务器、监视、管理、日志、配置、生成客户端以及关于等功能。如下图所示：

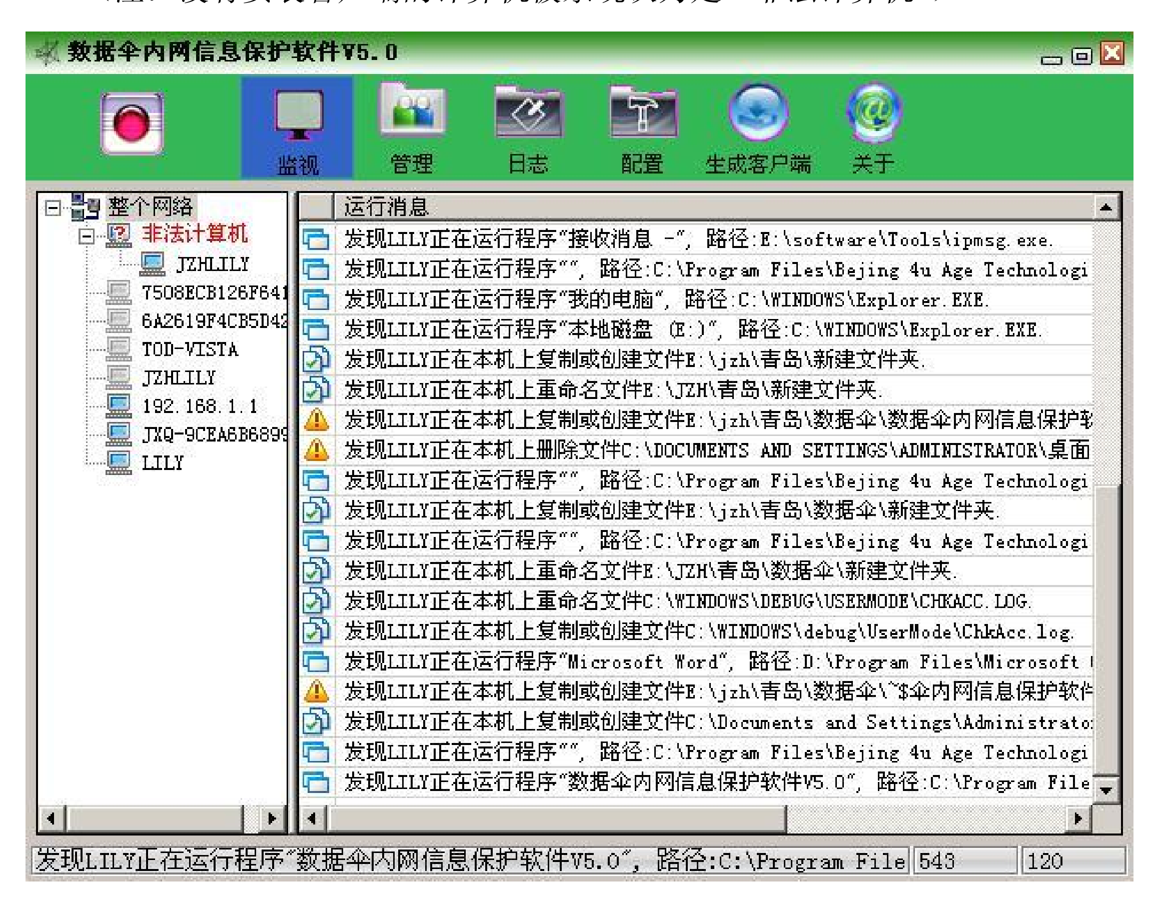


可分为三个操作区，**1.**操作区（上方的菜单条），**2.**操作区（左侧的树列表），**3.**操作区（右侧主区域）

4．2、监视菜单

监视整个局域网中所有主机或网络设备的接入情况，其信息包括用户名、IP地址以及是否合法等信息。在监视界面中，很直观的可以查询到哪些计算机终端有没有安装客户端程序外，还可以直接在操作区右侧里实时查看到当前网络内所有计算机的操作情况。如下图所示：

（注：没有安装客户端的计算机被系统认为是“非法计算机”）

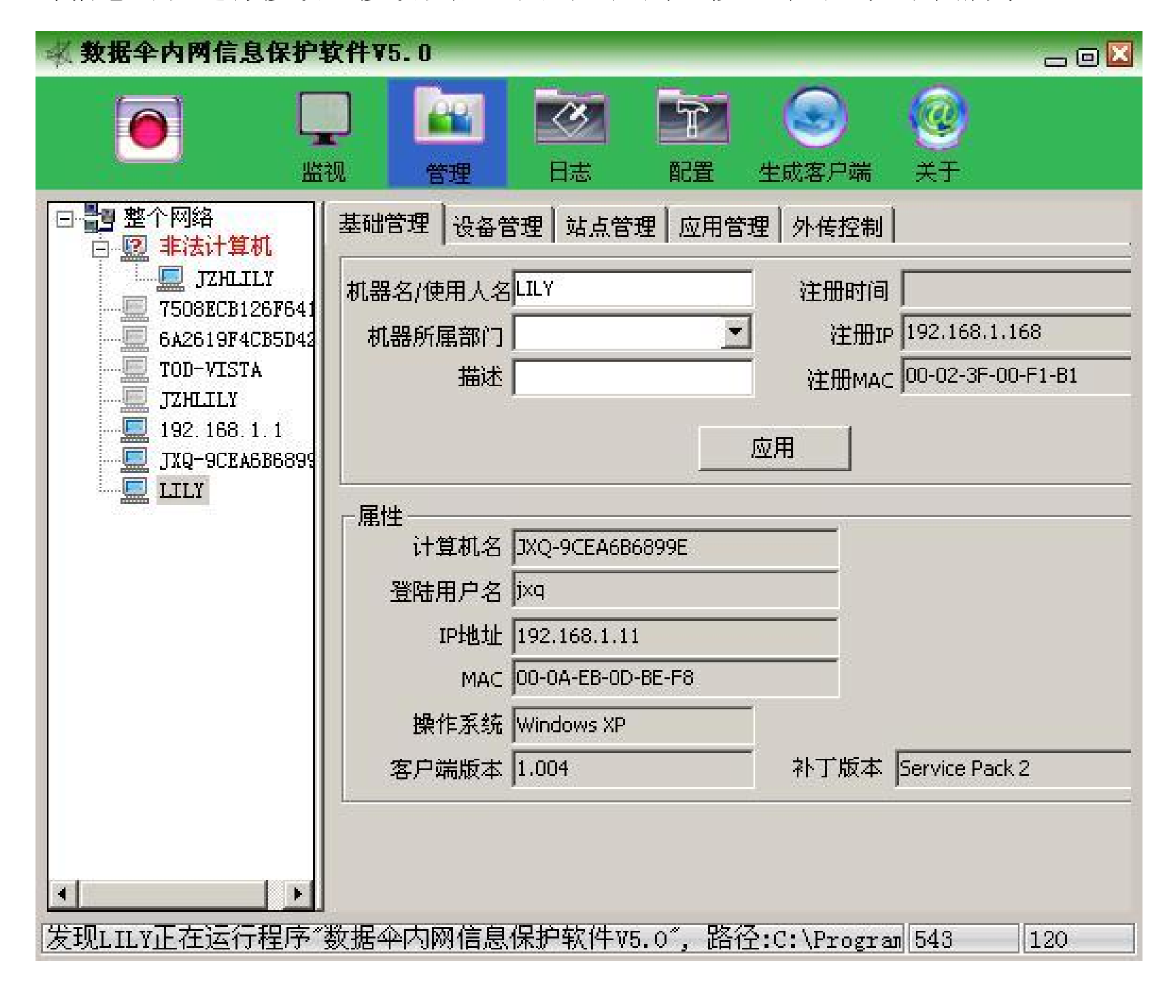


4．3、管理菜单

单击管理图标，可实现如下操作，

4.3.1、基础管理

可以对每台合法计算机终端基本信息进行管理，如：机器名、机器所属部门、注册 IP、注册 MAC 以及当前登陆用户名。其中，机器名、机器所属部门、描述等信息可以进行修改，修改以后，点击【应用】按钮即可。如下图所示：



4.3.2、设备管理

可以对每台合法计算机终端设备进行管理，如：串口、**USB** 存储设备、红外口、**ZIP**、软驱、光驱、**1394**、**Modem**、打印机等设备进行禁止和启用管理。

选择要禁止或启用的设备，点击【设置】按钮即可，在上面的设备记录列表框中很直观的可以看到当前设备的状态。如下图所示：

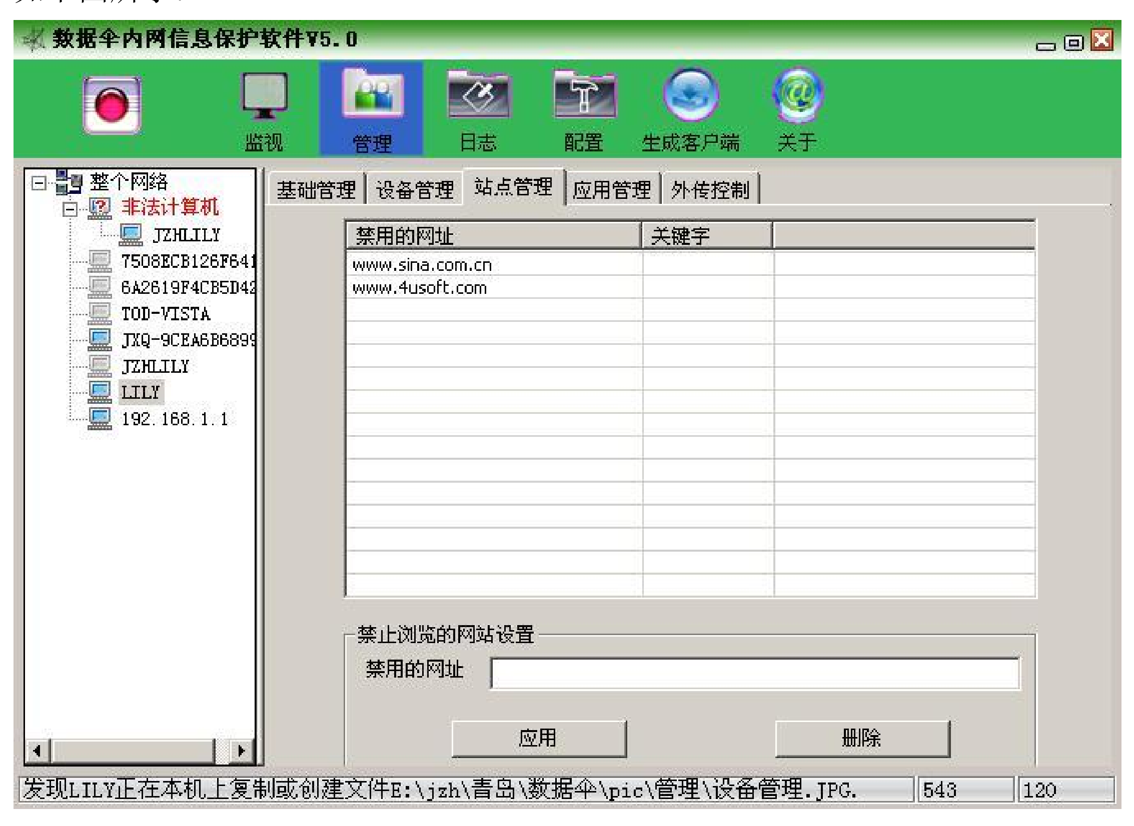


4.3.3、站点管理

可以对每台合法计算机终端禁止访问的站点进行管理。

在禁用的网址输入框中输入要禁止访问的站点，点击【应用】按钮即可禁止当前计算机终端不能访问该站点；

选择要禁用的站点，点击【删除】按钮即可开放当前计算机终端能访问该站点。如下图所示：

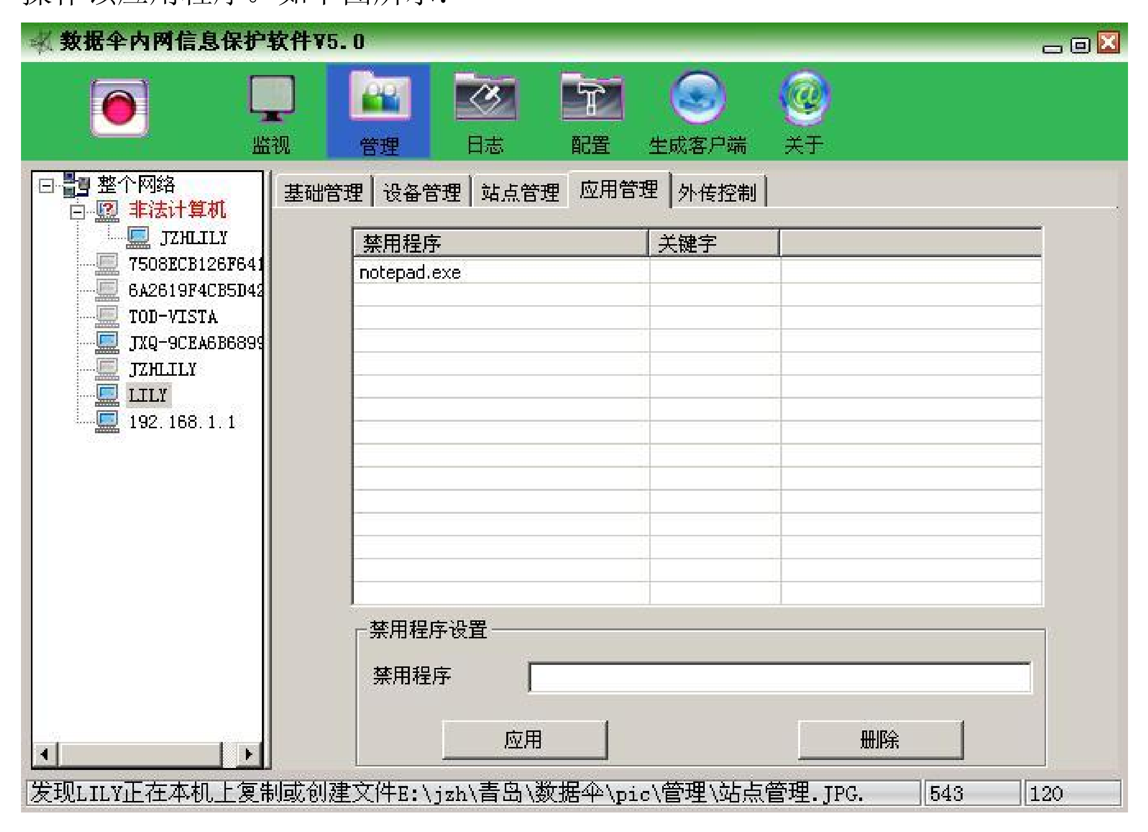


4.3.4、应用管理

可以对每台合法计算机终端禁止操作的应用程序进行管理。

在禁用的网址输入框中输入要禁止操作的应用程序，点击【应用】按钮即可禁止当前计算机终端不能操作该应用程序；

选择要禁止操作的应用程序，点击【删除】按钮即可开放当前计算机终端能操作该应用程序。如下图所示：



4.3.5、外传控制

可以对每台合法计算机终端文件外传方式进行管理。

选择要禁止的文件外传方式，点击“应用”按钮即可进行文件外传控制。如下图所示：



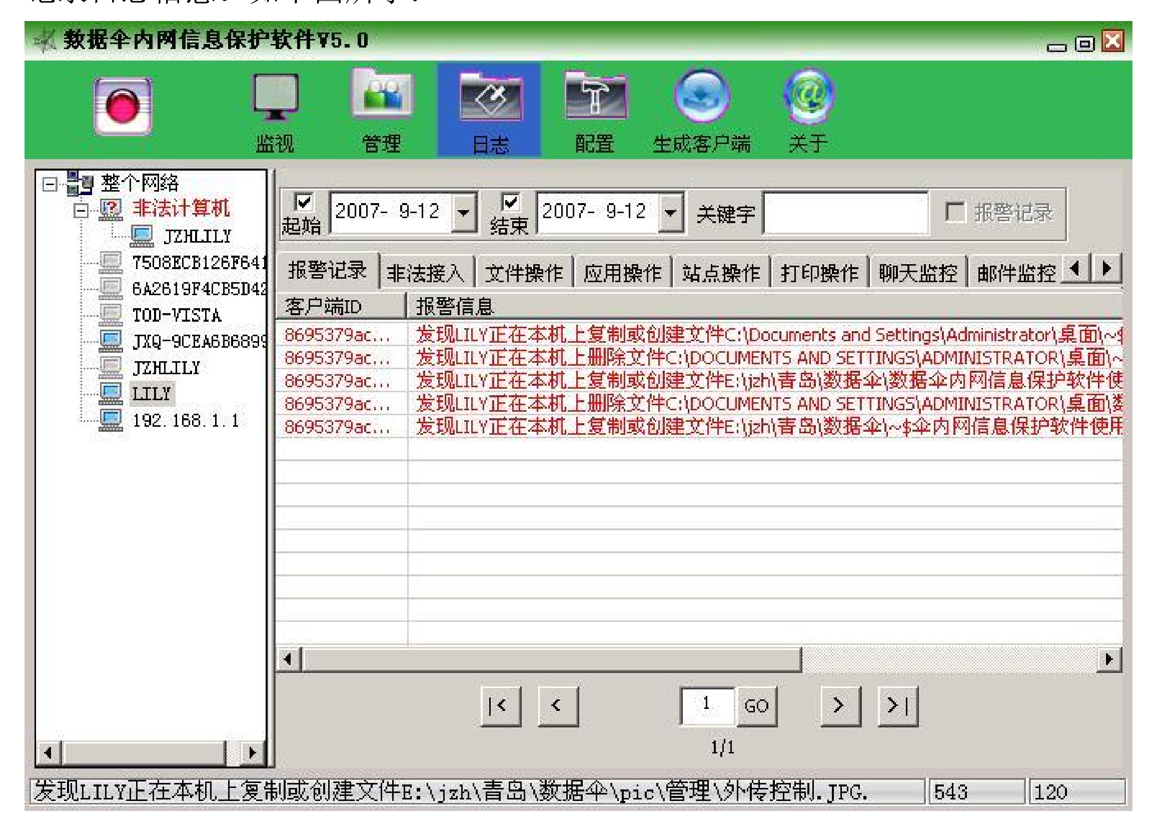
4．4、日志菜单

4.4.1、报警记录

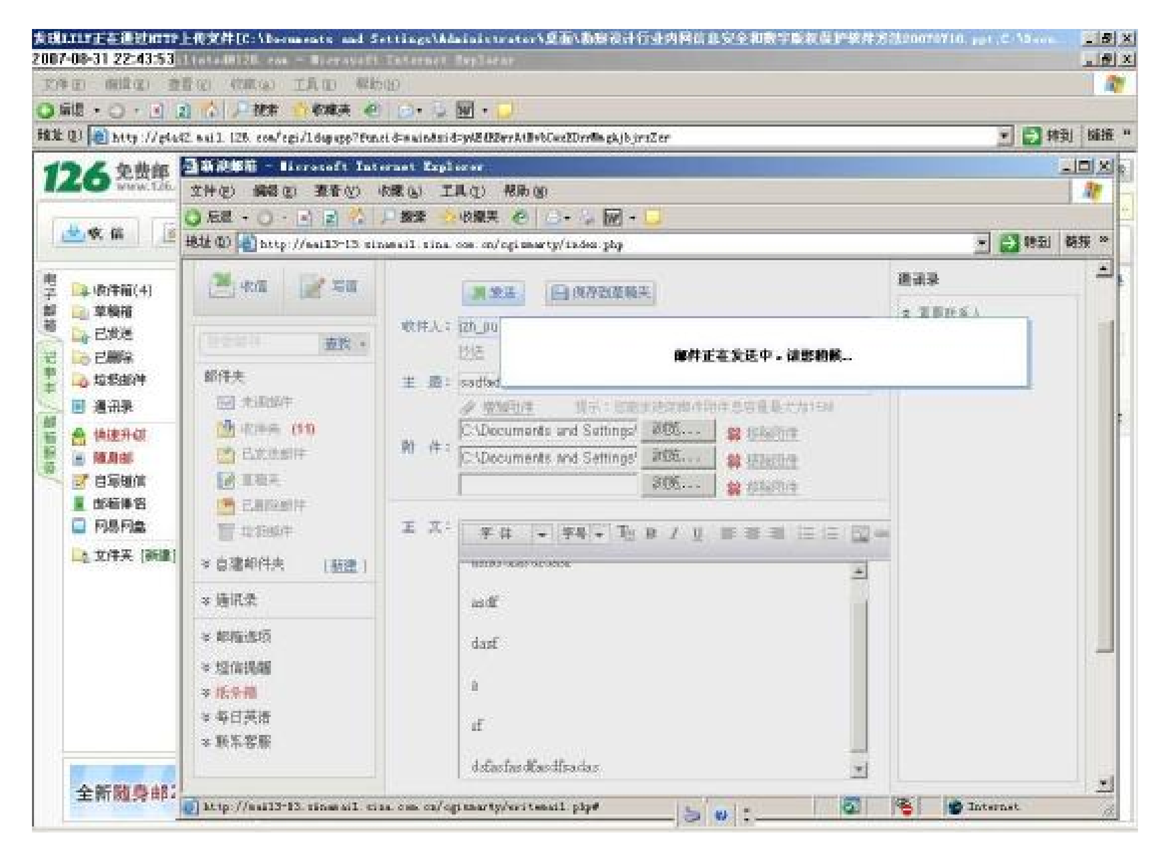
对非法接入、敏感文件操作等信息的记录，起到及时查询重要文件外泄记录作用。

报警日志记录信息包括：客户端 ID、报警信息、阻止状态、报警时间、接收时间等信息。

点击|<、<、>、>|按钮，查看到第一页、上一页、下一页、最后一页的记录日志信息。如下图所示：



选择某条报警记录，双击即可查看到客户端在操作文件的时候截图图片：



4.4.2、非法接入

计算机终端接入局域网进行记录。

非法接入日志记录信息包括：主机名称、主机 **IP**、**MAC**、设备类型、厂商、接入时间、离线时间等。

点击|<、<、>、>|按钮，查看到第一页、上一页、下一页、最后一页的记录日志信息。如下图所示：



4.4.3、文件操作

对每台合法计算机终端文件操作进行监控的记录。

文件操作日志记录信息包括：操作类型、文件名、操作人、操作进程、操作时间、源路径、目标路径等信息。

点击|<、<、>、>|按钮，查看到第一页、上一页、下一页、最后一页的记录日志信息。如下图所示：



4.4.4、应用操作

对每台合法计算机终端应用程序操作的记录。

应用操作日志记录信息包括：操作类型、程序名、程序标题、操作人、进程路径、操作时间等信息。

点击 |< 、 < 、 > 、 >| 按钮，查看到第一页、上一页、下一页、最后一页的记录日志信息。如下图所示：

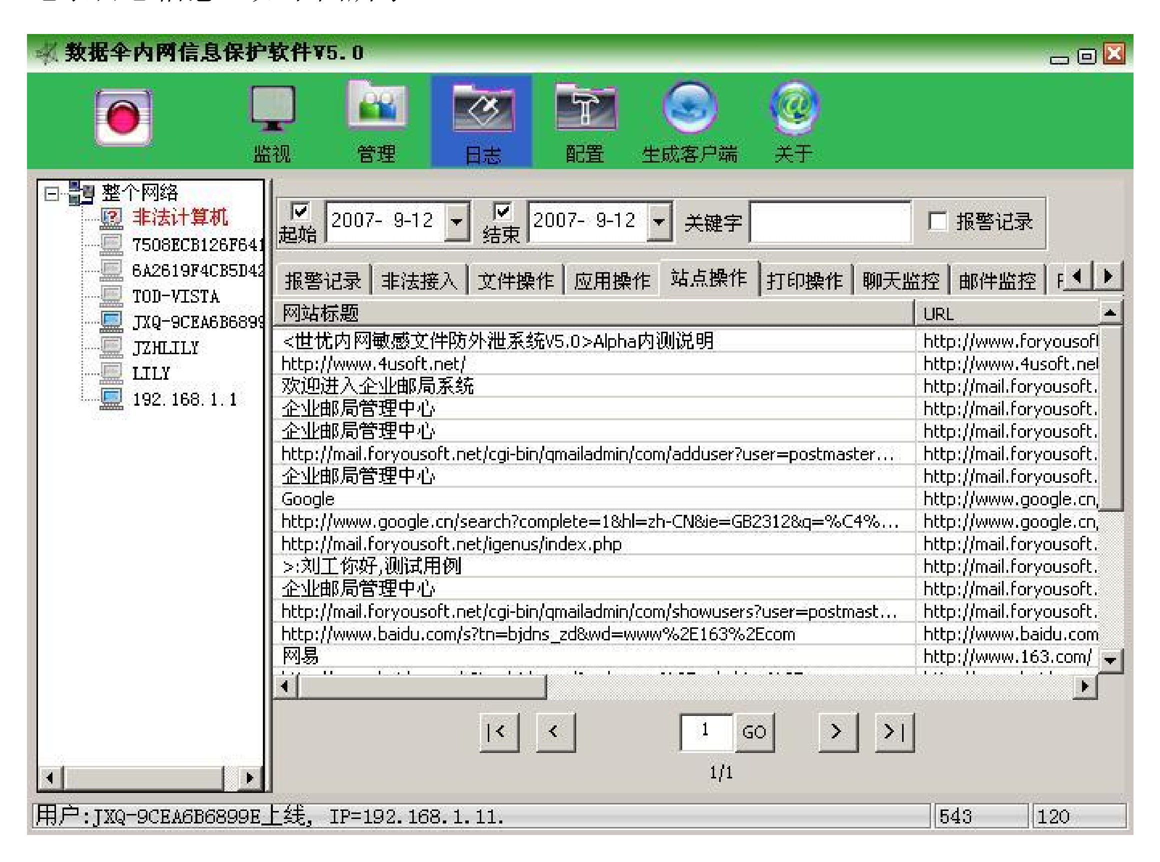


4.4.5、站点操作

对每台合法计算机终端站点访问的记录。

站点操作日志记录信息包括：网站标题、操作人、**URL**、操作类型、操作时间、接收时间等信息。

点击 |<、<、>、>| 按钮，查看到第一页、上一页、下一页、最后一页的记录日志信息。如下图所示：



4.4.6、打印操作

对每台合法计算机终端打印操作的记录。

打印操作日志记录信息包括：文件名、文件大小、页数、打印人、打印机名、打印时间等信息。

点击|<、<、>、>|按钮，查看到第一页、上一页、下一页、最后一页的记录日志信息。如下图所示：

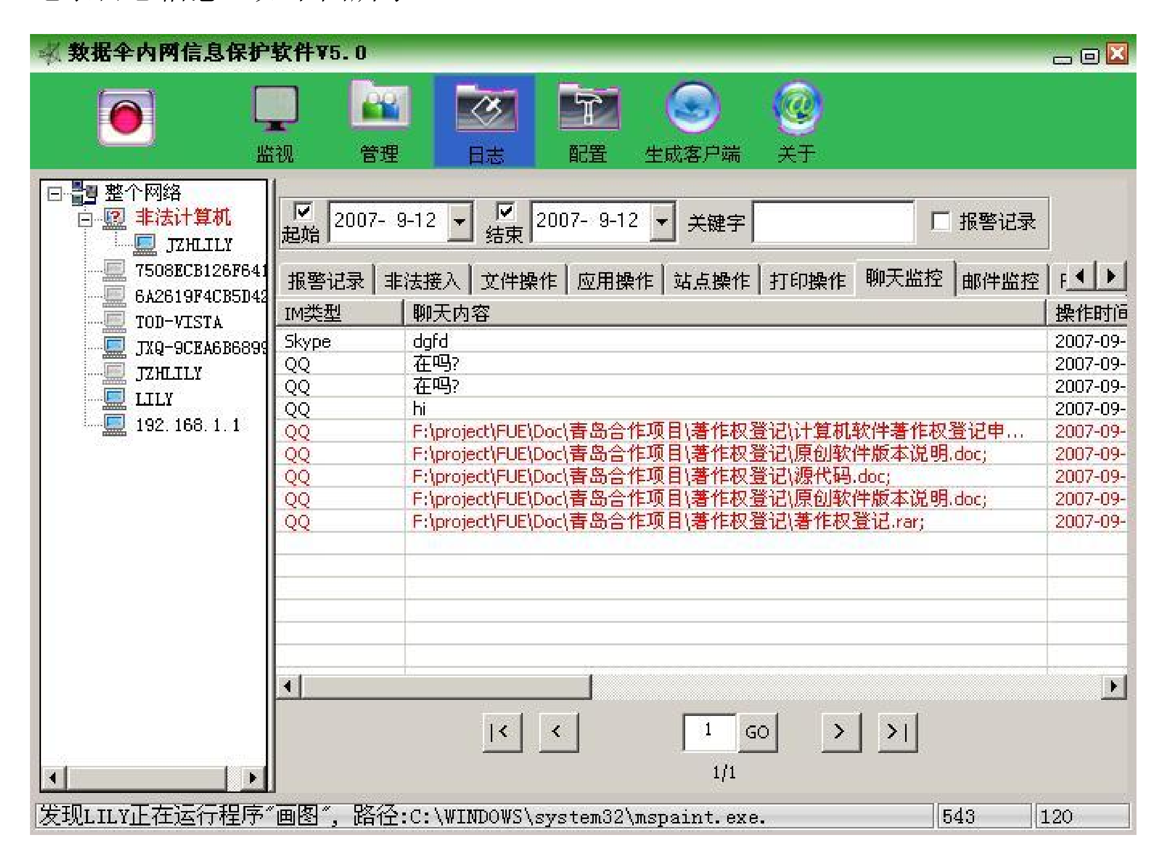


4.4.7、聊天监控

对每台合法计算机终端聊天监控的记录。

聊天监控日志记录信息包括：IM 类型、发送人、接收人、聊天内容、内容类型、操作时间等信息。

点击|<、<、>、>|按钮，查看到第一页、上一页、下一页、最后一页的记录日志信息。如下图所示：

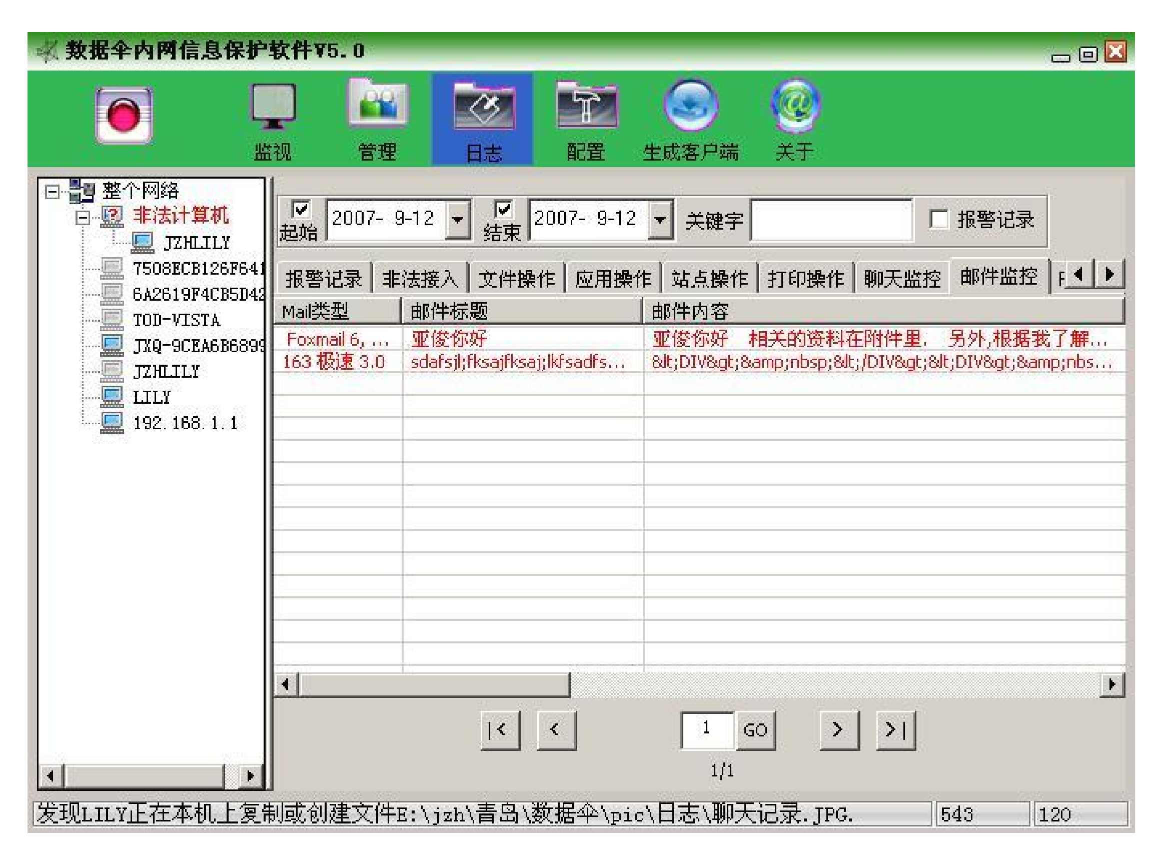


4.4.8、邮件监控

对每台合法计算机终端邮件发送和接受监控的记录。

邮件监控日志记录信息包括：**Mail** 类型、邮件标题、发送人、接收人、邮件内容、附件、操作时间等信息。

点击|<、<、>、>|按钮，查看到第一页、上一页、下一页、最后一页的记录日志信息。如下图所示：

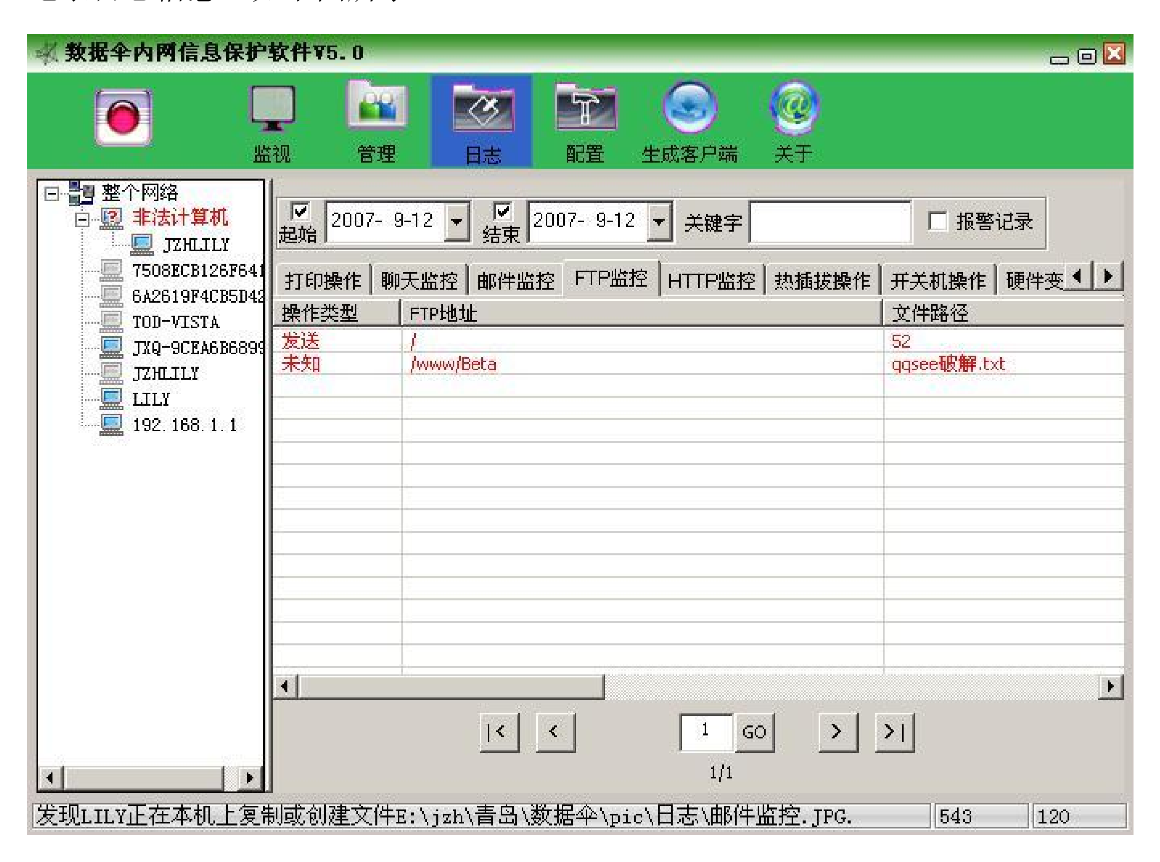


4.4.9、FTP 监控

对每台合法计算机终端 **FTP** 操作监控的记录。

FTP 监控日志记录信息包括：**FTP** 类型、操作类型、**FTP** 地址、文件路径、操作人、操作时间等信息。

点击|<、<、>、>|按钮，查看到第一页、上一页、下一页、最后一页的记录日志信息。如下图所示：

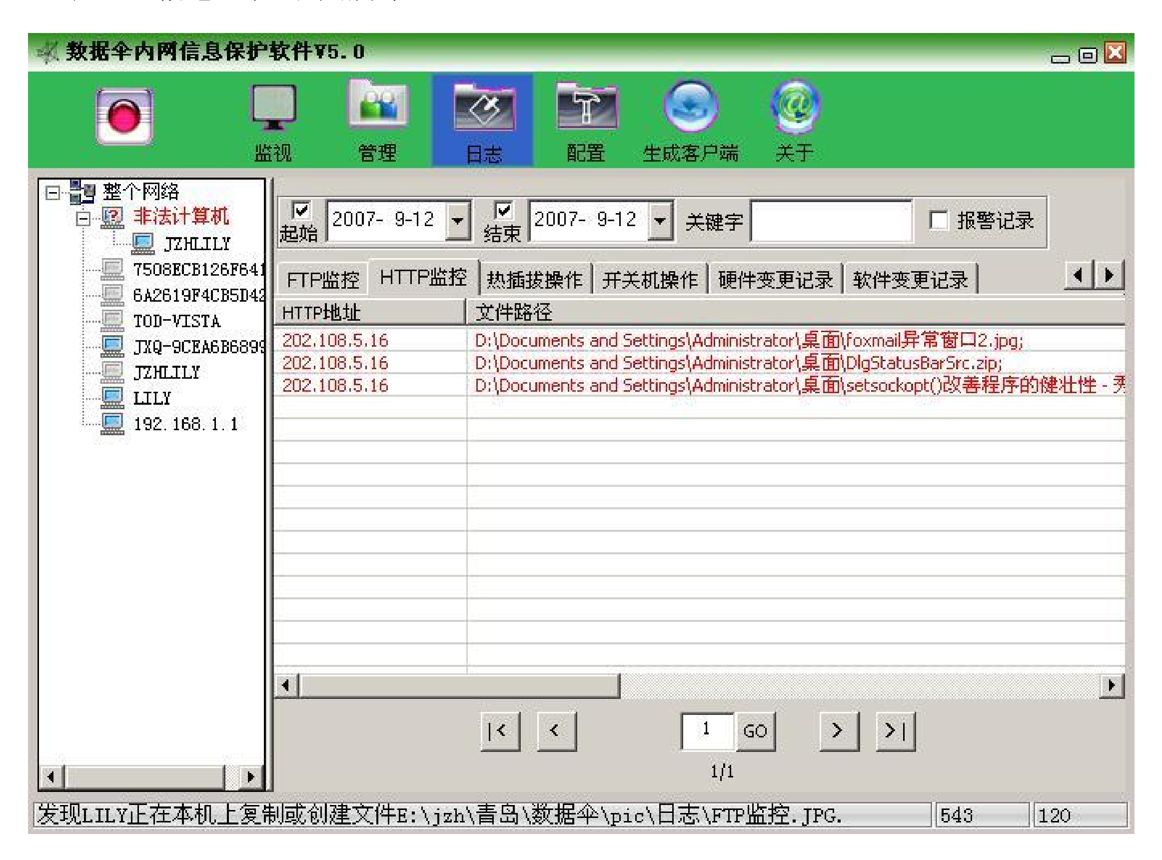


4.4.10、HTTP 监控

对每台合法计算机终端 **HTTP** 操作监控的记录。

HTTP 监控日志记录信息包括：**HTTP** 地址、文件路径、操作人、操作时间、报警信息等信息。

点击|<、<、>、>|按钮，查看到第一页、上一页、下一页、最后一页的记录日志信息。如下图所示：

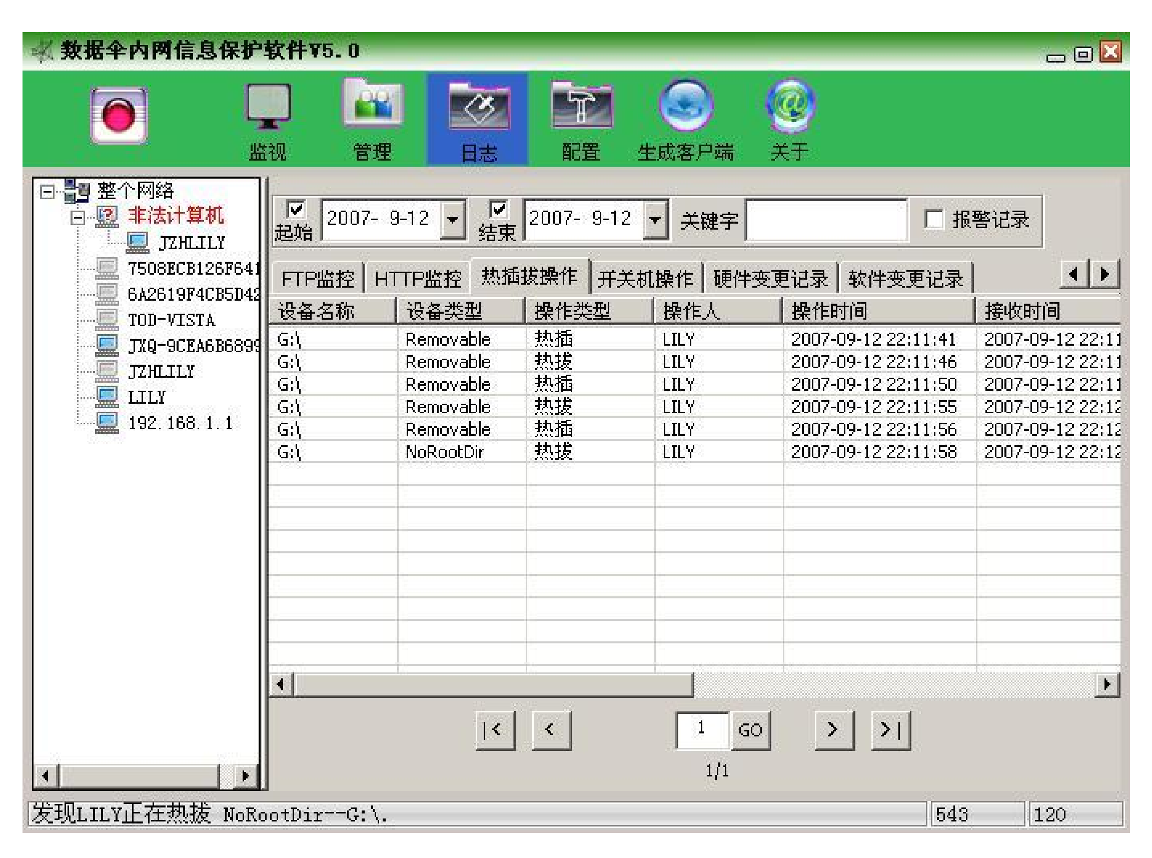


4.4.11、热插拔操作

对每台合法计算机终端热插拔操作监控的记录。

热插拔监控日志记录信息包括：设备名称、设备类型、操作类型、操作人、操作时间、接收时间、报警信息等信息。

点击|<、<、>、>|按钮，查看到第一页、上一页、下一页、最后一页的记录日志信息。如下图所示：

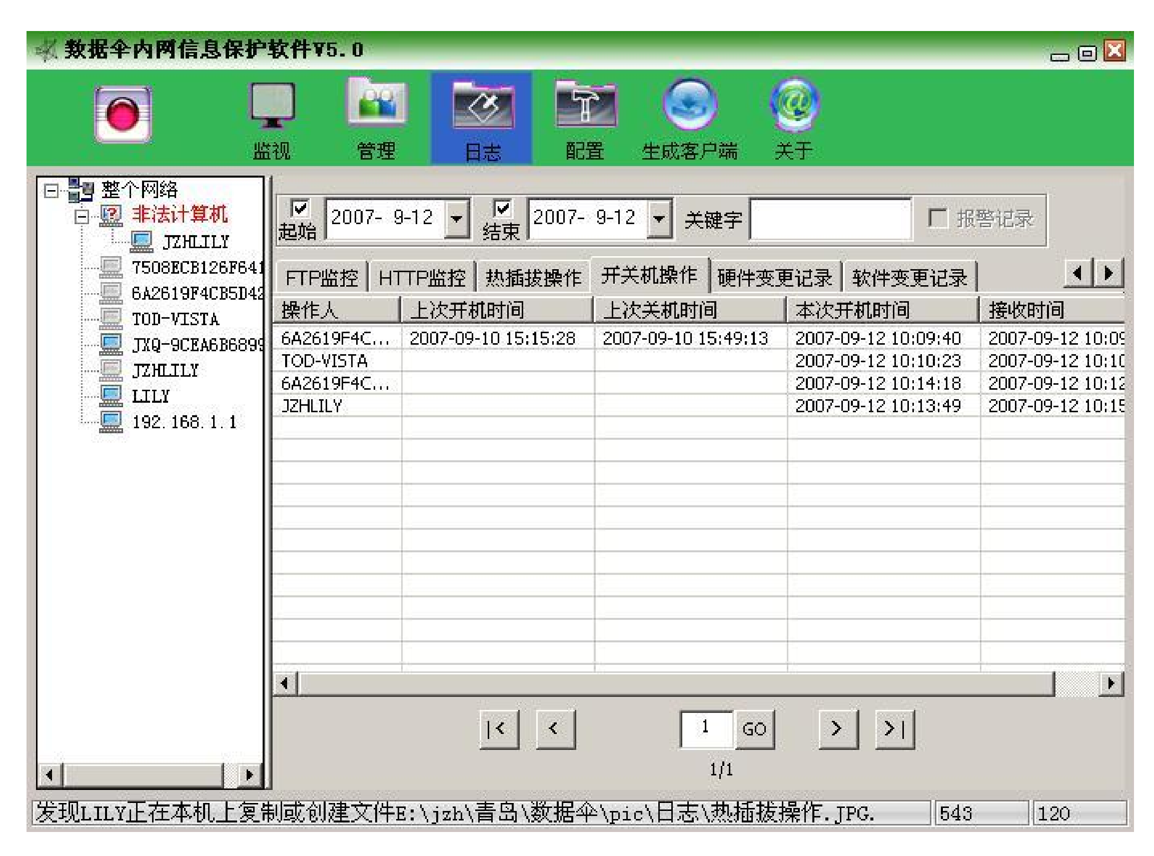


4.4.12、开关机操作

对每台合法计算机终端开关机操作监控的记录。

开关机操作日志记录信息包括：操作人、上次开机时间、上次关机时间、本次开机时间、本次关机时间、接收时间等信息。

点击 |< 、 < 、 > 、 >| 按钮，查看到第一页、上一页、下一页、最后一页的记录日志信息。如下图所示：

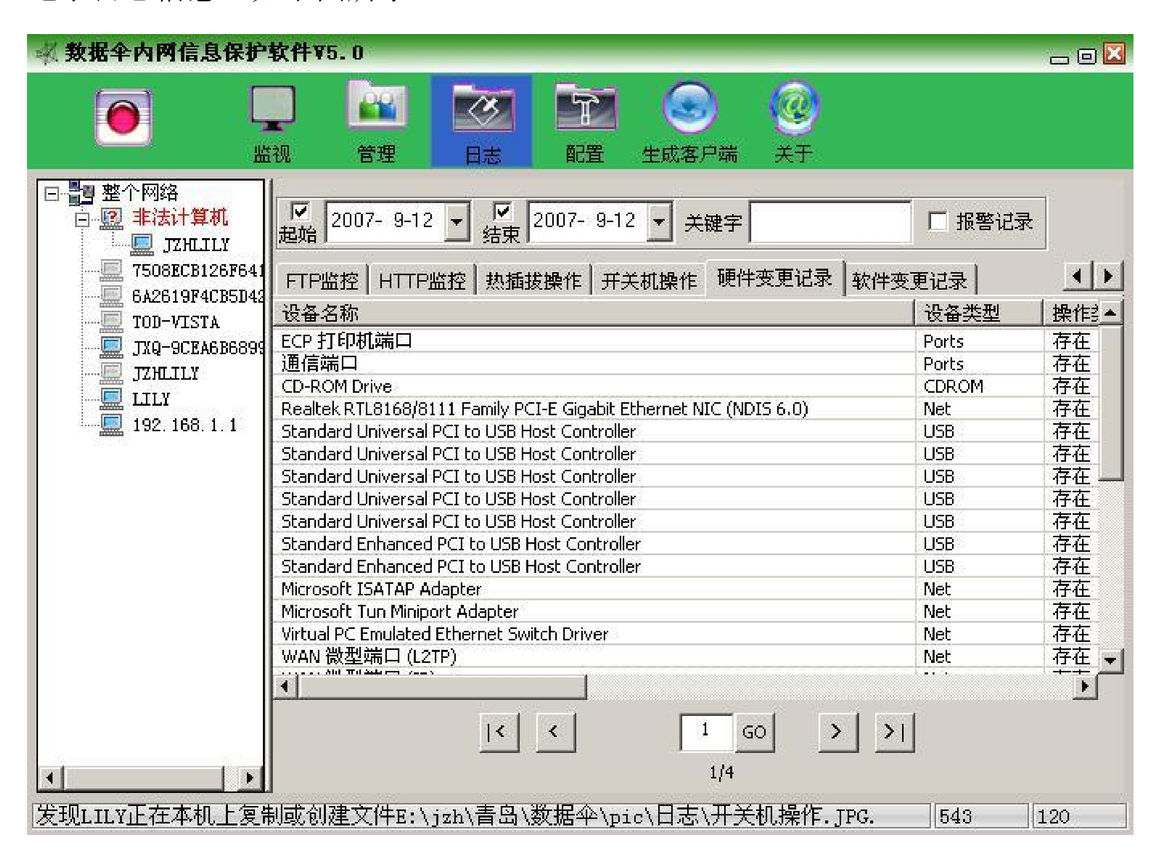


4.4.13、硬件变更记录

对每台合法计算机终端硬件变更的记录。

硬件变更日志记录信息包括：设备名称、设备类型、操作类型、操作人、操作时间、接收时间、报警信息等信息。

点击|<、<、>、>|按钮，查看到第一页、上一页、下一页、最后一页的记录日志信息。如下图所示：



4.4.14、软件变更记录

对每台合法计算机终端软件变更的记录。

软件变更日志记录信息包括：软件名称、软件版本、操作类型、操作人、操作时间、接收时间等信息。

点击|<、<、>、>|按钮，查看到第一页、上一页、下一页、最后一页的记录日志信息。如下图所示：



4．5、配置菜单

4.5.1、网络扫描：

对合法 IP 和扫描网段等进行设置。

l　合法 IP 设置：

在 IP 地址框中输入要进行合法 IP 地址的 IP、MAC 地址、IP 描述，点击【应用】按钮，即可添加成功；

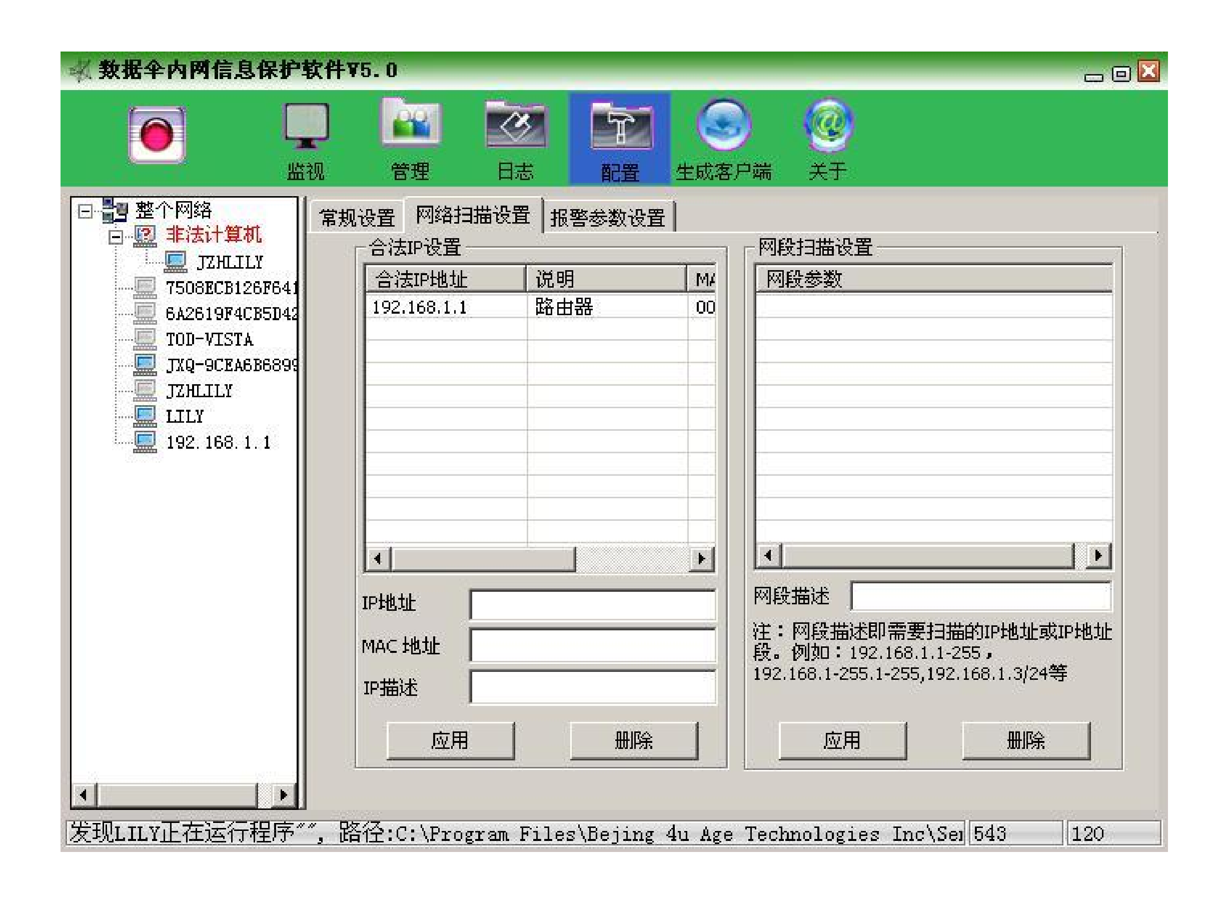
选择要删除的 IP 地址，点击【删除】按钮，即可删除设置的合法 IP 地址；

l　扫描网段设置：

把需要扫描的 IP 地址或 IP 地址段添加到扫描列表中，点击【应用】按钮，即可添加成功；网段描述例如：**192.168.1.1-255**；**192.168.1-255.1-255**；**192.168.1.3/24** 等。

选择要删除的扫描网段记录，点击【删除】按钮，即可删除设置的扫描网段；

如下图所示：



4.5.2、报警参数设置

对文件名关键字报警、标题关键字报警、Mail/IM 关键字报警等参数进行设置。

- 文件名关键字报警设置：

在文件名关键字报警输入框中输入要进行报警的文件名关键字，点击【】按钮，即可添加成功；

选择要删除的文件名关键字，点击【】按钮，即可删除成功；

- 标题关键字报警设置：

在标题关键字报警输入框中输入要进行报警的标题关键字，点击【】按钮，即可添加成功；

选择要删除的标题关键字，点击【】按钮，即可删除成功；

- Mail/IM 关键字设置：

在 Mail/IM 关键字输入框中输入要进行报警的 Mail/IM 关键字关键字，点击【】按钮，即可添加成功；

选择要删除的 Mail/IM 关键字，点击【】按钮，即可删除成功；

- 文件外传形式报警设置：

选择文件外传报警形势，比如 U 盘文件拷出报警、邮件外传文件报警、FTP 外传文件报警、HTTP 外传文件报警、IM 外传文件报警等，点击【应用】按钮，即可设置成功。

如下图所示：


数据伞内网信息保护软件V5.0
监视
管理
日志
配置
生成客户端
关于
整个网络
非法计算机
JZHLILY
TOD-VISTA
JZHLILY
LILY
192.168.1.1
常规设置
网络扫描设置
报警参数设置
文件名关键字报警
包括硬盘文件、FTP、HTTP、Mail、IM、打印等
报警的关键字
合同
方案
设计
财务
.doc
.dwg
计划
标题关键字报警
包括网页浏览标题、应用程序标题等
报警的关键字
程序员
求职信
公司
基金
股票
游戏
Mail/IM关键字报警
包括发送的Mail内容、IM内容
报警的关键字
法轮功
TMD
U盘文件拷出报警
邮件外传文件报警
FTP外传文件报警
HTTP外传文件报警
IM外传文件报警
应用
发现LILY正在本机上复制或创建文件E:\jzh\青岛\数据伞\pic\配置\Thumbs.db:encryptab
543
120

4．6、生成客户端程序菜单

在服务器端可以直接方便的生成客户端程序，点击主菜单栏中的【生成客户端】按钮即可，客户端的安装请参考上面描述的客户端安装说明。

4．7、关于菜单、软件自动升级

在关于界面中可以查看到数据伞内网信息保护软件的服务器端版本、版权所有以及所有客户端升级等信息。

软件自动升级

点击“导入升级包”按钮，选择客户端升级包或直接将升级包拽入关与界面中即可对所有客户端程序进行升级。如下图所示：



4．8、单台终端操作

4.8.1、基本管理

可以对所选的合法计算机终端基本信息进行管理，如：机器名、机器所属部门、注册 **IP**、注册 **MAC** 以及当前登陆用户名。其中，机器名、机器所属部门、描述等信息可以进行修改，修改以后，点击【应用】按钮即可。具体请参考“管理菜单”中的“基本管理”。

4.8.2、设备管理

可以对每台合法计算机终端设备进行管理，如：串口、**USB** 存储设备、红外口、**ZIP**、软驱、光驱、**1394**、**Modem**、打印机等设备进行禁止和启用管理。具体请参考“管理菜单”中的“设备管理”。

4.8.3、站点管理

可以对每台合法计算机终端禁止访问的站点进行管理。具体请参考“管理菜单”中的“站点管理”。

4.8.4、应用管理

可以对每台合法计算机终端禁止操作的应用程序进行管理。具体请参考“菜单管理”中的“应用管理”。

4.8.5、外传控制

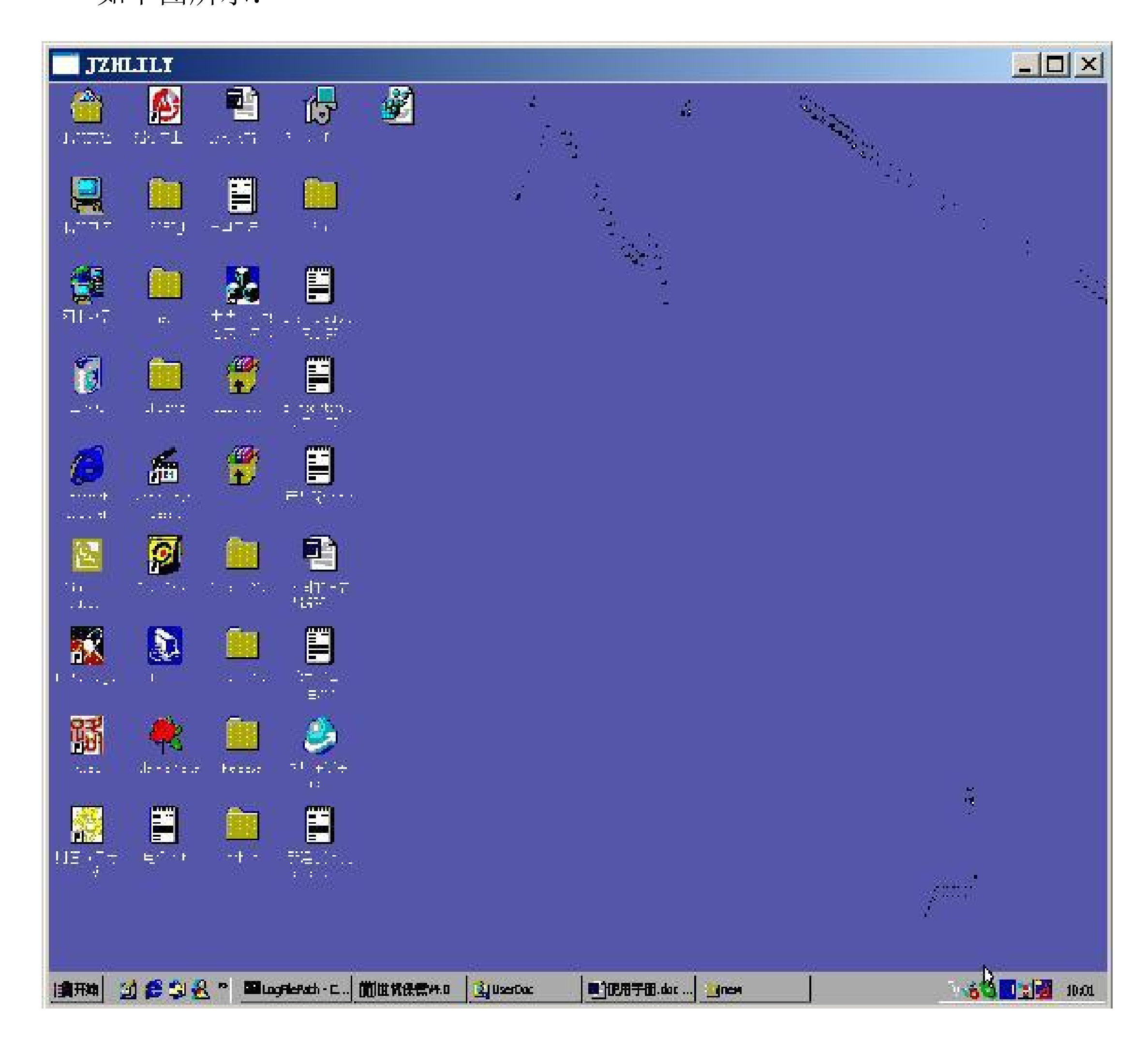
可以对每台合法计算机终端文件外传方式进行管理。具体请参考“管理菜单”中的“外传控制”。

4.8.6、远程控制

选择单台合法计算机终端，右键选择远程控制。

可以对每台合法计算机终端远程进行控制，可以远程操作计算机终端。

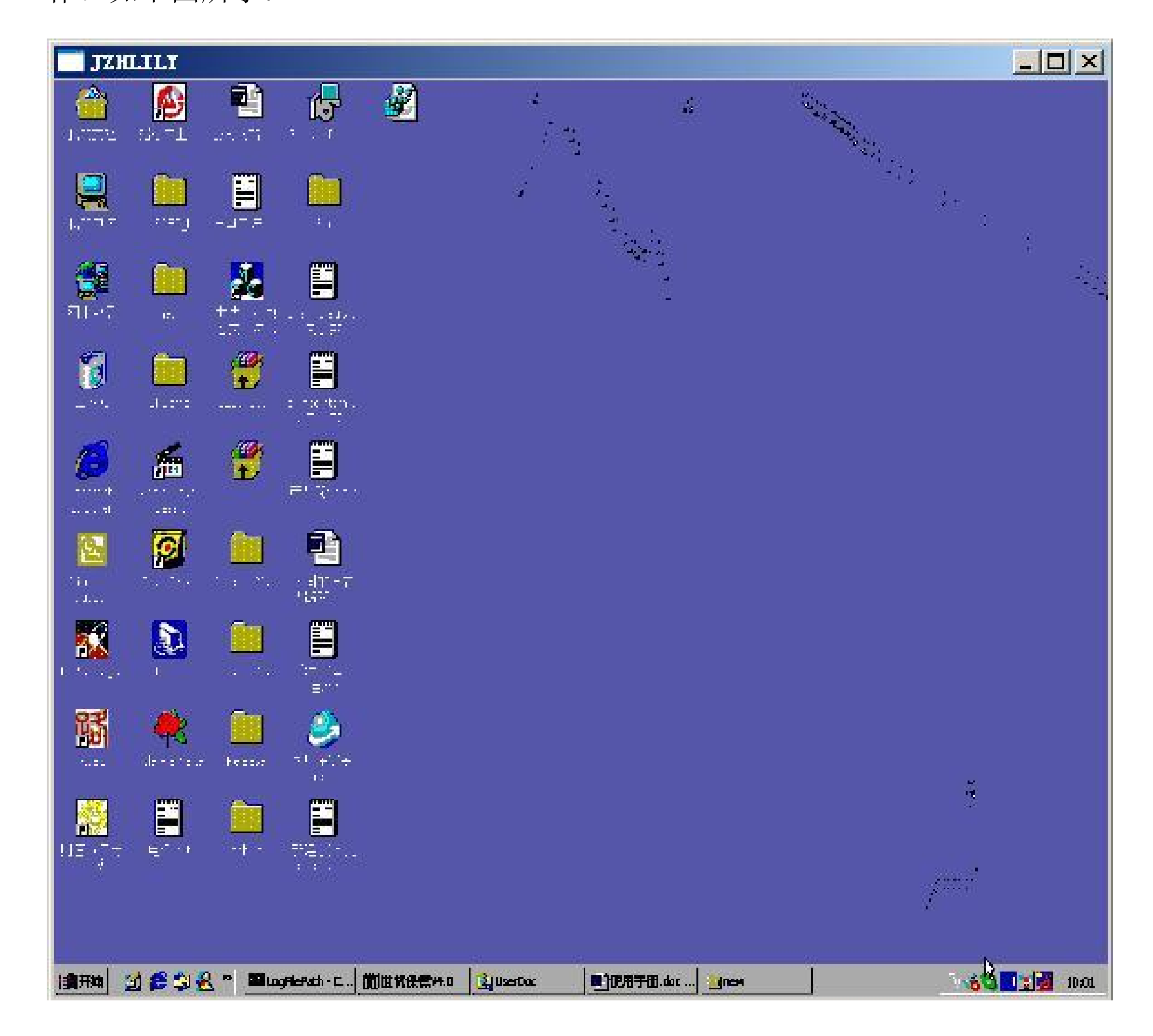
如下图所示：



4.8.7、远程屏幕监视

选择单台合法计算机终端，右键选择远程屏幕监视。

可以对每台合法计算机终端远程屏幕监视，可以远程查看到计算机终端操作。如下图所示：



4.8.8、远程截屏

选择单台合法计算机终端，右键选择远程截屏。

可以截取每台合法计算机终端当前操作的屏幕图片。

五、常见问题

1．数据伞内网信息保护软件支持那些操作系统？

答:操作系统支持,**Windows2000,WindowsXP,Windows2003**等。

2．数据伞内网信息保护软件的安装需要满足什么网络方面的条件么？

答：我们的系统不需要您对网络进行任何形式的改造，局域网内部无论通过何种形式联网，或者通过何种形式上网，我们的软件这方面都没有要求。

3．客户端将网线拔了，软件是否还起作用？

答：客户端将网线拔了，他的所有操作依然处于被监控的状态，只不过服务器端无法连接该客户端，下次客户端网线插入后，服务器端可以看到客户端端在网线拔了之后这段时间的所有的操作。